Toward a National Security Architecture Prepared for Information Warfare

CSC 1995

Subject Area – National Security

EXECUTIVE SUMMARY

Title: Toward a National Security Architecture prepared for Information Warfare

Author: Mark K. Ward, LCDR, USN

Research Question:

How can the National Security apparatus be restructured to meet the challenges and opportunities that Information Warfare presents?

Discussion:

The U.S. leads the World in the information "sciences" but organization, policy and doctrine are not keeping up with technology in either the military or governmental sectors. The lag not only disallows the U.S. from taking advantage of new technological developments, but makes the U.S. vulnerable. An overarching structure that is flexible, lean, and responsive is needed to provide coordination between all of the "producers" and "users" of Information Warfare (IW) support. The synergy that would result from DOD and non-DOD governmental organizations coordinating operations across the "information spectrum" would greatly increase the overall security of the U.S.

Conclusions:

The greatest progress is occurring in DOD, therefore IW must first be refined there, shown to be successful, and migrated throughout the U.S. Government. The first step in the process outside of DOD should be to square away the National Security apparatus. Next, protection of the industrial and civilian sectors will need to be provided for. the new information technologies that are emerging will require a very close look at the Constitution. Laws, policies and oversight bodies will be required so that the protection of individual and corporate rights are balanced with the need to counter the threat of Information Warfare. The requirement to respond to the threat posed by IW, and the resulting efficiencies gained in the process, will transform

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
1995

2. REPORT TYPE

3. DATES COVERED
00-00-1995 to 00-00-1995

4. TITLE AND SUBTITLE
Toward a National Security Architecture Prepared for Information Warfare

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Marine Corps War College,Marine Corps Combat Development Command,Quantico,VA,22134-5067

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**49**	

the civilian society, and change the way the U.S. military is organized and fights.

CONTENTS

Napoleon Bonaparte said, "The battlefield is a scene of constant chaos. The winner will be the one that best controls that chaos, both his own and that of his enemy." Napoleon might judge the advances in Command, Control, Computer, Communication and Intelligence (C4I) technologies in recent years to be a grand opportunity, for both the US and its potential adversaries. U.S. C4I prowess has contributed to great success in recent years, such as that seen in the Persian Gulf war. Harnessing advances in C4I before an adversary can is the essence of Information War (IW), the ongoing battle to limit ones own information chaos while contributing to or exploiting an adversary's chaos. A National Security **Architecture**[1] that includes IW concerns will ensure the U.S. continues to enjoy information dominance in peacetime or war. This paper will discuss how the U.S. can update its existing National Security Architecture to respond to the challenges and opportunities IW presents.

WHAT IS A NATIONAL SECURITY ARCHITECTURE?

The term "structure" has historically been used to describe the relationships between and within organizations charged with a particular function or mission. MBA students have studied organizational structures in the past but as computers and information systems have swept into all parts of modern life, the students now study architectures or relationships. The word "structure" can connote rigidity, while the information age meaning of the word "architecture," as one envisions a computer program flowchart, better describes the fluid relationships that have to exist within any successful, efficient organization in today's competitive world. U.S governmental organizations that are tasked with National Security can be no less flexible and responsive than civilian high technology companies. While the issue may seem to be a matter of semantics to some, the responsiveness issue is really about mindsets and paradigm shifts.

The very real threat that IW poses is pervasive and can be manifest in minutes. The IW threat does not afford the defender long lead times to counter it. For example, during the Cold War, the discovery of a new weapon the Soviets may have planned to field eight years hence could be reacted to. IW changes all past concepts of time and space. U.S. sovereignty and property can be attacked in the next moment from anywhere by anyone with a computer modem. A National Security "Architecture" that is capable of winning the Information War every moment is needed.

There now exists a National Security Structure that is incomplete and somewhat dysfunctional, with a semi-formal Architecture that is inadequate. The Structure and Architecture are inadequate because they are too reactive in nature, which will suffice against enemies that fly at sub-mach speeds to drop weapons, drugs, or contraband on US territory, but against the stealthy, insidious, lightning threat that IW represents, more responsiveness and constant vigilance is needed. The National

Security Structure will require time for staff study and legislation, but the problem can be stemmed with an interim Architecture that is aggressive with respect to the IW threat. In other words, it must be proactive and intrusive with respect to adversary systems while remaining impregnable to the most talented hacker, professional criminal, or foreign country.

WHAT IS INFORMATION WARFARE?

Due to the relative newness of IW as a concept, much of the work is classified. IW terminology is only now becoming standardized within U.S. Governmental circles. Open source writings on IW are still interlaced with the hard to understand slang of "Cyberpunk" publications. Cottage industries have sprung up to serve the new subcultures who wander "Cyberspace" or world "information superhighways." There is a great deal of excitement about the endless possibilities that new found systems, such as Internet, hold for the U.S. and the world. Some of the excitement is hype, similar to that seen at the beginning of the personal computer age, when manufacturers sought to encourage families to buy personal computer's to put recipes on diskette; however, just as the value of personal computers became clearer over time, the possibilities of IW are becoming clearer with every news headline describing a thwarted attempt to electronically rob or manipulate a data base. A discerning professional tasked with U.S. National Security concerns should examine IW for the real challenges and opportunities it presents. The challenges include protecting increasingly vulnerable U.S. information pathways, while the opportunities include preventing undesired domestic and international events through attainment of near perfect intelligence upon which appropriate actions can be taken. In an austere environment, overreaction must be avoided, but an expedient, but measured and steady approach is needed to incorporate IW tactics, techniques and procedures into National Security organizations, individually and collectively.

For the purpose of this paper, Information Warfare (IW) will be the term used for the broadest view of the new field, while the strictly military applications of IW are called Command and Control Warfare (C2W). Much of the current IW thought has gone on at National Defense University (NDU) and the Joint Staff, the latter concentrating on C2W. While the Joint Staff has not published doctrine or even a definition for IW, it has distributed a second draft doctrine for C2W and has great appreciation for IW. The reason for this seeming incongruency of having a subset of a warfare approach maturing before the overall concept, is quite simply that the basic tenets of C2W (operational security/deception/early warning/psychological operations/physical destruction) have been practiced for many years by DOD and defense-related non-DOD entities, mainly in wartime. IW is a newer, larger concept, which to a greater extent involves peacetime and economic issues. IW is described as a concept because it is still taking shape and only now being recognized by the whole of the National Security Community for the paradigm shifts it will require and continue to require, as the rest of this paper will describe. IW is a silent killer with no rules of engagement. IW changes the nature of warfare because it is pervasive and omnipresent. Warning time in IW is nil because the enemy only needs a modem and phone line to softkill your operation. The enemy (or your ally) could be (metaphorically) staring at you through the screen you are typing into. IW goes beyond the C2W actions, many of which are rudimentary and have been practiced for years, yet are still essential.

While advances in technology have been the major contributing factor, "IW" also came into being because of the influence of 1986 legislation to promote jointness and the idea that a seamless DOD C2W effort would gain effectiveness through synergy. Technological advances created unconventional opportunities for both the U.S. and its potential adversaries. NDU has been empowered to move forward with the IW concept as executive agent, and to teach IW seminars for senior defense and governmental community players until a broader national IW concept and architecture can be negotiated between DOD and many other governmental entities (e.g. CIA, State, Treasury, and Interior Departments). NDU uses the following definition of IW that has heretofore found favor with a broad audience:

> ***...an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. IW is both offensive and defensive in nature -- ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability and interoperability of information assets. While ultimately military in nature, IW is also waged in political, economic and social arenas***

> ***and is applicable over the entire national security continuum from peace to war. Finally, IW focuses on the command and control needs of the commander by employing state of the art information technology and synthetic environments to dominate the battlefield.*** **NDU IW STUDENT HANDOUT**

5

The Joint Staff has defined the strictly military applications of IW, or C2W, as follows:

> ***The integrated use of operations security (OPSEC),military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to,influence,degrade, or destroy adversary command and controlcapabilities,while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the range of military operations and all levels of conflict. C2W is both offensive (counter-C2) and defensive C2-protect). The goal of C2-protect is to maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade or destroy the friendly C2 system. The goal of counter-C2 is to prevent effective C2 of adversary forces by denying information to, influencing, degrading or destroying the adversary C2 system.*** **Joint Pub 3-13**

WHY IS IW IMPORTANT?

IW can contribute significantly in any operation. As the U.S. leads the world into the 21st century, what threats, challenges and opportunities face the country? Depending on how U.S. political leaders come to see national interests, the country could be involved in a wide range of actions. The threat of IW to U.S. information systems in peacetime alone is significant enough to warrant a reworking of American National Security Architecture. The peacetime IW threat is now, and will remain, a constant danger that is arguably more serious a consideration than the more traditional IW missions, such as jamming a communication frequency or radar during an airstrike. A disruption in Wallstreet trading by a hacker or fanatic/terrorist would have severe repercussions around the world. The first and most important capability in the future will be to ensure friendly communications and systems are secure. The U.S. federal and state governments, and the American public and industries must become more aware and act to counter potential threats.

IW actions must go beyond peacetime considerations of OPSEC, to missions such as PSYOPS in Operations Other Than War (OOTW), or selective Command and Control (C2) destruction through nodal analysis in Major Regional Conflicts (MRC). While the possibility of conflict in Korea or Iran cannot be discounted, the predominant types of military operations for the foreseeable future will be OOTW. Preparedness for IW in an MRC goes a long way toward readiness for IW in OOTW and vice versa, as the major difference is the degree of physical destruction involved. These OOTW missions may involve combat and non-combat missions, to include peace keeping and enforcement, counter drugs/contraband/proliferation/terrorism, and others. No matter what the operation, IW is integral because at a minimum it involves the protection of friendly information management capability. Even a peaceful disaster relief or nation building mission will require the U.S. to manage and protect its communication abilities. The figure below describes the near universal utility IW (from Joint Pub 3-13/figure II-3).

IW APPLICABILITY IN OPERATIONAL CONTINUUM

Range of Peacetime Ops	OPSEC------------------>	OOTW
Range of Military Ops	OOTW------------------->	War
Levels of Conflict	Tactical--------------->	Strategic
Disciplines	Offensive-------------->	Defensive
Planning Cycle	Crisis----------------->	Deliberate
Size of Force	Platoon---------------->	Multi-Corps
Composition of Force	U.S. ----------------->	Multinational
Rules of Engagement	Restricted------------>	Unrestricted
Geography/Terrain/Weather	Jungles--------------->	Deserts
Opponents	Allies---------------->	Arch enemies
Techniques Available	SIGINT---------------->	Destruction

The extent to which the U.S. can gather inteligence on increasingly sophisticated opponents, disseminate necessary information to decision makers, and manipulate control of that which is available to a potential or actual adversary will grow geometrically in importance. IW capability will grow in importance much faster than even the projected technological advances in precision guided weapons (PGM) and stealth technologies, which were so successful in the Persian Gulf war. The new opportunities, and conversely the new vulnerabilities, lie in the realm of IW.

Peacetime decisionmakers must have the information necessary to influence events, thwart terrorist acts, stop WMD proliferation, or predict opponent negotiating positions on decision points. The future wartime Commander must, in near-real time, be able to see all of his forces on the battlefield and take advantage of U.S.

intelligence dominance to coordinate the use of lethal and nonlethal weapons to effect mission success with near impunity. The American public demands "no-hitters", which requires steady investment in the technological advances that will allow a leaner force to prevail in those future situations that the U.S. government hopes to influence. Today's theater, joint force, or civilian Commander needs what a powerful IW concept can give, the ability to get inside the enemies observation, orientation, decision and action cycle (or "OODA loop").[2]

A bold IW capability cannot be supported by the existing National Security Architecture. The current Architecture is inefficient, inadequate and already vulnerable. DOD and non-DOD organizations are not operating in conjuction for a variety of reasons. No coordinating oversight body has ever provided effective leadership. These organizations function together only because dedicated men and women use secure phone lines to conduct liaison on known issues of mutual interest; they're systems are not tied together and they lack synergy. Additionally, many systems of the National Security Architechture are "stovepiped," preventing DOD and non-DOD organizations from efficiently sharing information and working together. Stovepiping exists when an organization or system exists for a single or few purposes, and uses an inordinate amount of assets for the extremely specialized purposes it accomplishes; conversly, the absense of stovepiping inmplies an asset able to accomplish much more for less. Stovepiping has persisted because of incompatible information handling systems and databases, lack of incentive and strong Joint leadership, fear of change, and the vestiges of overrestrictive security measures from the Cold War which still hamper information exchange. Another contributing factor to American unpreparedness for IW is that information pathways procurred for the National Security Architecture have inadequate capacity to support a robust IW effort.

The National Security Architecture is vulnerable because only the most classified systems are adequately protected. Some of the most important American security concerns are embodied in the protection of files of defense contracters, not those at CIA, NSA, or FBI. Increasingly frequent reports of various individuals hacking their way into less well defended U.S. systems suggests a rising sophistication that endangers U.S. information security. The security stakes and monetary costs of ineffiecency and inadequacy are too high to continue to respond to the challenges and opportunities of IW this way.

CHALLENGES AND A VERY BRIGHT FUTURE

The U.S. dominates the world in all aspects of the use and management of information. Primarily the dominance has occurred in civilian applications because Government use of new technology has always lagged the civilian environment. American industries still lead in computer development and are unchallenged in software. Innovative spirit and an inventive nature are American characteristics that have kept the U.S. on top in information management in a fast changing and competitive world. The U.S.

military, and National Security organizations in general, however, resist change until stressed, and they weren't stressed quite enough in the last conflict.

There were problems with aspects of IW during Desert Shield/Desert Storm (DS/DS). The problems were visible to insiders, but not to the media, which fed a proud public a steady stream of cockpit footage of Precision Guided Munitions (PGM) destroying targets. Fortunately, Iraq turned out to be inept in IW/C2W and most Coalition problems involved the efficient use of its own communication systems. The largest problem was that U.S. Architecture was inefficient with the inadequate bandwidth available. Adaptations and workarounds were sometimes required to make communications functional, and it wasn't very reassuring. For example, many in the military are familiar with how slow routine to immediate message traffic became because of competing flash (highest level) precedence traffic that clogged information transfer "arteries." The problem came with multi-section messages, which kept being preempted by flash traffic; a major message system that connected DOD and non-DOD organizations would simply restart at the beginning of a preempted message and new messages would continue to que-up. Soon, another flash message, perhaps regarding a SCUD warning, would delay the system again. In frustration, those sending msgs would increase the precedence of their traffic in order for it to arrive on time, which further compromises the fidelity of the system. Huge messages like the Air Tasking Order (ATO), the daily "blueprint" by which all aircraft conduct their

missions, had to be physically flown out to a Navy carrier from the

Joint Forces Air Component Commander (JFACC) HQ at Riyadh, Saudia Arabia to ensure proper coordination. There were other similar problems, like systems not being able to transfer data due to lack of interoperability, but the positive thing is the U.S. still dominated in IW.

The media feeding frenzy surrounding "lessons learned" was largely unsuccessful at defining any major failures, although it made a run at fratricide and the time-honored scape goat, intelligence. As a result of the IW/C2W abilities not being severely stressed and no major faults publicized following DS/DS, National Security leaders have been slow to move. Greater mental energy has been spent on justifying plans for "rightsizing" than on IW. The U.S. National Security Architecture can't wait for stress or failure, to whatever degree, to be the agent of change. Decision-makers must recognize that there are not only solutions to problems, but great opportunities in IW/C2W if the energy and appropriate asset prioritization is afforded it. This is a hard sell because IW is primarily a supporting function, not about riveting cockpit footage, but it is all about ensuring cockpit success.

The opportunities lie in a new level of power to shape a situation, mindset or battlefield so that U.S. leaders need only act on near perfect intelligence to quickly settle many issues. No other military in history has ever had near perfect intelligence and own force situational awareness, and U.S. technology is fast

approaching the capability to field such an Architecture. Sun Tzu said "know thine enemy and thine self and you will win every battle." Add near perfect intelligence and the own force situational awareness which will come with a functional IW Architecture, with new generations of PGMs, and the resulting conventional power advantage the U.S. will possess will be near absolute over any foe in any regime of conflict.

Additionally, the ability IW will bring to unconventional challenges like terrorism and the drug war will be devastating. Imagine not being three steps behind Iranian sponsored terrorism or the Cali Cartel but in its face, or perhaps two steps ahead. "Messages" could be sent or perceptions modified via IW through unconventional IW activities. The messages could be as covert as manipulting data so that the computers controlling a refinery or nuclear "research" facility cause a damaging explosion, or as overt as manipulating an adversarial Nation's media. Imagine what these acts might do to the minds of leaders who would otherwise attempt terrorists acts. Many might be convinced to play by the rules and work within the international system through negotiation. Many of the problems responsible powers are fretting about in Sudan, Algeria and Egypt could fade.

IW has incredible potential and offers the U.S. a brighter, more secure future. That more secure future will require the U.S. National Security Architecture better keep up with IW related C4I capabilities being marketed. The turnaround time for C4I technology in industry is about eighteen months, vice DOD average

of approximately seven years to field a weapon system. The U.S.

must develop a security "culture" that is always looking outward for IW threats in the marketplace, and willing to be flexible in procurement so that IW security can be maintained. Advanced Concept Technology Demonstrations (ACTDs) using prototypes must be utilized to test new systems.

REORGANIZING NATIONAL SECURITY FOR IW/C2W

The IW threat requires interim action in the form of Presidential Directives. Presidential directives established NSA and DIA years after the 1947 National Security Act; the same decisive action is needed now to provide interim guidance while the 1947 Act can be reworked. A task force led by a senior executive branch person should be empowered to review new requirements with those governmental organizations involved with National Security. The review should result in possible courses of action for the President to act on. These courses of action should identify and seek to rectify current impediments to progress toward a viable National Security Architecture. Current impediments include the lack of articulated relationships between all the IW participants, equipment and data bases that are not interoperable, lack of doctrine or tactics, techniques and procedures, legal questions, and a general lack of appreciation for the IW threat.

The President's National Security Adviser and his staff would be the appropriate leadership of a body tasked to work on an interim National Security Architecture; the body would include select members and staff of the Senate and House Armed Service

Committees, Senate Select Committee on Intelligence (SSCI) and

House Permanent Select Committees on Intelligence (HPSCI), the National Foreign Intelligence Board (NFIB), and traditional (CIA, DIA, etc) and non-traditional (Commerce, Justice, etc) National Security Organizations. From the HPSCI and SSCI should be formed a legislative oversight committee to provide continuous monitoring and chairmanship duties when the National Security Advisor is unavailable; this committee would form the cadre to continue work toward a new National Security Act.

DOD OUT IN FRONT

DOD has led other National Security Organizations in public recognition of the importance of IW/C2W and has set about to reorganize accordingly. CIA, FBI and NSA have long used aspects of IW but have operated individually and kept operational efforts and funding classified. In contrast, the Services have cooperated at the tactical level and are better suited culturally to forward IW. DOD has historically practiced the basic functions of IW/C2W (deception, etc) but also participated in classified National efforts through Tactical Exploitation of National Capabilities (TENCAP). DOD has become a leader because the publicity surrounding greater funding for IW and desire to coordinate the IW/C2W efforts of the Services under Joint auspices has brought more attention to the subject.

Assuming it can be believed that the U.S. is at the forefront of the IW/C2W race, so far as is currently known, how does it shore up present inadequacies and stay ahead? The following paragraphs

will discuss the areas where progress is needed and where some plans have been made. The changes will involve procurement and a significant and evolving, preferably long term reorganization of DOD and non-DOD National Security Organizations. The changes must first occur in DOD, which is the largest single National Security Organization, with a built-in, strong coordinating leadership in OSD and JCS that is able to push through the needed changes. As DOD approaches proper calibration, the IW culture should be migrated to other National Security Organizations.

The first step in the process outside of DOD should be to tie together the remaining organizations, responsible primarily for internal U.S. National Security. Next, protection of the industrial and civilian sectors will need to be provided for. While outside the scope of this paper, the author recognizes new information technologies that are emerging will require a very close look at the Constitution. Laws, policies and oversight bodies will be required so that the protection of individual and corporate rights are balanced with the need to counter the threat of Information Warfare.

Reorganization of the National Security Architecture would not only ensure preparation for IW, but also result in greater efficiencies, energy and effectiveness in providing for total U.S. security.

SYSTEMS MUST BE SEAMLESS

One of the largest hurdles to overcome in the development of a U.S. IW architecture is that both DOD and non-DOD programs have

historically attempted to maximize systems for their own needs.

This is especially true of DOD, and to a lesser degree, non-DOD organizations that use more Commercial Off The Shelf (COTS) technology. Only since the demise of the Soviet Union, and the attendant search by elements of the National Security Structure to look for ways to justify their size or even existence, has greater cooperation between the elements been emphasized. Security concerns and more than enough work to go around contributed to maintaining the status quo; different organizations had different security rules and there was institutional fear that if something was lost or leaked, careers would be lost. With so much work to do, and little emphasis on exchange other than publication or message traffic, short term coordination issues were deemed "too hard." Most coordination between DOD and non-DOD organizations still occurs via secure phone, but people are thinking, planning and talking. New technology, the threat of consolidation with another organization or worse, and more time to think because the Cold War is over, have brought on paradigm shifts. The U.S. military, and DOD in general, is out in front due to the strong central leadership exerted by the Joint Staff. It should be mentioned that of the non-military elements of national security apparatus, the Central Intelligence Agency (CIA) and the National Security Agency (NSA) have had tremendous success in IW/C2W; however, the nature of those independent agencies is unlikely to allow them to be leaders in the development of an overarching IW architecture. The cultures of CIA and NSA remain

decidedly covert in outlook and neither can compare, to use a joint phrase, to the "preponderance of forces" brought to the effort by DOD. Additionally, DOD has the large staff required to see such a large undertaking to fruition. DOD's early successes in implementing the tenets of IW/C2W, will lead the way for the rest of the government; however, there is much remaining to accomplish in C2W.

The main challenges lie in the C2-protect area, specifically, having **secure** communication and data display/manipulation/transfer systems that will talk to each other. The security needed for communications are different than those needed for data storage and manipulation. Communications are discrete bursts of energy that can be recorded by the enemy, and given powerful enough computing power, any crypto can be broken eventually. Thus, protection from a sophisticated foe intent on reading a targeted transmission that he can physically capture, cannot be thwarted; however, the defending party can, by powerful hardware and software, delay the crytoanalysis so that the traffic is of less value. For extremely sensitive transmissions the defending party must guarantee security by moving communications to other means, like low-probability-of-intercept Satallite Communications (SATCOM). SATCOM, for example, is expensive and cost prohibitive for large volumes of traffic. A great deal of work is ongoing in defense and industry to expand the capabilities of SATCOM. A technological advance like the use of multiplexing, or time sharing fiber optic phone lines based on sensors that connect random transmitters and recievers when a user

talks, makes SATCOM more economically feasible and changes the C-2 protect equation. Protection of data is more challenging and an area where less emphasis has been placed. The U.S. is now becoming aware that a database or network of databases is only as secure as the least capable system connected. A talented attacker can enter a moderately protected system. A few brilliant people have entered some very well protected defense and banking systems, without the use of highpower computers that might aid in breaking the code for password entry. New computer software warns if a system is being attacked, but in a recent U.S. attack the perpetrator was able to accomplish his goal so fast that he outmaneuvered the protection. Noted IW writer and speaker Robert Steele believes there is value in recruiting and hiring such talents to ensure they work on the side of good. In any case, to stay ahead of potential adversaries in C-2 protect, the U.S. must invest in new communications-related technologies and stay on par if not ahead of the competition.

There are considerations in the C2-attack arena as well, like the need for coordinating attack methods so that fratricide does not occur. For example, if the enemy is using a particular communication frequency you would like to use, or use to listen to him, coordination is needed to ensure the frequency is not jammed or interferred with.

These problems in both C2-attack/protect are both hardware and software related, but are not insurmountable; they only call for definitive, aggressive management according to a joint plan. The plan is embodied in the Joint Staff's Global Command and Control System (GCCS). Although the DOD programs (mainly the military services) pay homage to the need to conform to GCCS plan, progress has been painfully slow due to legitimate service-specific requirements for future systems, adaptation to "legacy" (mature operating) systems, and lack of incentive to do the very difficult and expensive coordination and acquisition required.[4] The coordination and acquisition is difficult and expensive because all of the requirements of the participants must be taken into account. In past decades, several Joint aircraft and missile programs have been cancelled because the participants couldn't compromise. Strong leadership was needed but no mechanism was in place.

A powerful direct influence is needed to tie together today's systems as quickly as possible, but also those being fielded and developed. A SECDEF task force studied this issue, recommending in October 1994 that the Battlefield Information Task Force (BITF) become permanent and provide liaison within DOD to ensure adherence to the GCCS plan and coordinate other IW initiatives. The sage Undersecretary of Defense for Command, Control, Communications and Intelligence, Emmit Page Jr., noted that the J-6 organization had been created in 1979 to do the same thing recommended to be done by the BITF. A different and potentially more successful approach would be to use the Joint Staff's reinvigorated Joint Requirements Oversight Committee (JROC) to coordinate issues such as this. The JROC, chaired by the Vice Chief, has recently moved toward becoming much more involved in coordinating and overseeing service procurement, and is currently reviewing IW initiatives as one of

its top future interests. Aggressive JROC involvement in IW development, especially at this early stage, would undoubtably yield quick, positive results and provide impetus for further JROC involvement in joint coordination issues.

With respect to non-DOD systems, the same challenges exist. System standards are needed to allow cross talk within and between DOD and non-DOD organizations. This is a very important issue because herein lies the lost unity of effort. Tie systems together and professionals can, for instance, "pull" from other databases what they need or don't even know. The synergy from this mid-range goal would provide a phenomenal improvement.

A computer system can only be as resistant to compromise as its weakest link. Consider a system tied together between non-DOD and DOD organizations. If information is to be shared in the future, and it must be, an invader could conceivably break into any participant database, then pass into another. For example, in the drug war, DEA and the Justice Department may request information of the Office of Naval Intelligence (ONI) on a suspect U.S. merchant ship. Currently, the request and information is limited to being passed back and forth via secure phone, for technology and legal reasons. (The U.S. military can't be involved in spying on Americans and ONI/DEA/Justice data-handling systems will not interact). Wouldn't the transfer of information be more efficient if the data bases could be shared? Time spent coordinating between various analysts could be spent more productively. How much useful information is not discovered or used because information is not

shared efficiently? The answer to this question will be known when systems can talk to each other and requisite security measures are in place. The security measures will be expensive. Physical security is important but each link of a reworked National Security Architecture will require the same level of electronic security. For example, if it is known that the Russians, or even the competitive French, Germans or Japanese, have a certain computing power, the U.S. had better have a more powerful one creating encryption against the possible attempt at entry in any point of the U.S. system.

The military is leading the way in the sharing of data bases. Military data bases are moving to a "pull down" vice "push" philosophy, where users can obtain what they want instead of large messages being sent to them. The previous method of "shotgunning" background and current information to a theater would swamp point to point communications, and give the recipient a headache trying to sift through the delayed and irrelevant information. The Military Integrated Intelligence Data Base (MIIDS) is the best example. It can be accessed through a JDISS (Joint Defense Intelligence Support System)[5] terminal via satellite communication from anywhere in the world. The problem is that JDISS has only been provided to joint commands, or the theater level. JDISS is a Navy-developed system and it is the only Service with a sufficient number of terminals to make the system feasible at the Service level. While the other Services have bought one or two terminals for some of their headquarters, the full capability of the system

has not been realized. This situation is a prime example of where an aggressive JROC, acting on behalf of the Joint Staff, could guide the services toward a better functioning information architecture.

EMPHASIZING THE CINC's

Before Goldwater-Nichols and the gradual transfer of power to the Joint Staff and the CINC's, the Cold War had dictated an information architecture that served the National Command Authority. It has become evident that Information Architecture must be readjusted to emphasize theater CINC (Commander IN Chief) or CJTF (Combined Joint Task Force) while still maintaining sufficient support to the top rungs of decisionmaking.[4] The Commander needs total enemy and friendly situational awareness, with the ability to impart this information in a timely manner and in a format tailored to each level of command. The information must have the appropriate security but not be encumbered to an extent that it becomes so time-late as to be of little or no advantage.

Existing architecture will not currently support a CINC or Joint Force Commander (JFC) that desires to exploit the current and developing capabilities of IW, as was clear in DS/DS. In DS/DS it became apparent that insufficient satellite access and bandwidth limitations were a hindrance. The inefficient distribution of message traffic via point to point communications made the overall communication system dangerously slow. Flash traffic was sometimes not, and priority traffic became so delayed that many commands

marked more routine traffic as priority hoping for it to arrive so as to be useful. We cannot do this again. Fortunately, there are fixes that can be quickly added while Research, Development, Testing and Evaluation (RDT&E) continue. One Architecture modification that shows great and immediate promise is to use the broadcasting mode to disseminate information. The idea is not new. Data links like Navy Tactical Data System (NTDS) or intelligence broadcasts have been sent periodically via HF in the past. Better technology promises to make this method an efficient means to send certain types of information.

IW/C2W CENTERS OF EXCELLENCE

Recognizing that the C2W warfare area required what in Total Quality Leadership (TQL) parlance is called a "center of excellence," CJCS established the Joint Command and Control Warfare Center (JC2WC) in September of 1994. Establishment of the JC2WC was a first in that no other warfare area has ever had a "Joint Center" established for the purpose of coordinating between the services and geographic CINC's, all aspects of a particular warfare area.[6] This was a significant milestone on several accounts. Most importantly, it shows that DOD/JCS recognize that IW/C2W are high priorities. It also signals a continuation of a process toward greater jointness between the services begun in 1986; DOD/JCS will lead the services toward a desired end state with respect to research, development, testing, evaluation and procurement in new warfare areas and challenges. The JC2WC is likely the prototype for future DOD/JCS organizations that, in consonance with the Joint Doctrine Center recently established in Norfolk, Va., will be influential in defining future warfare challenges and possibly redefining traditional warfare areas (i.e. ground warfare or air warfare).

LEGAL QUESTIONS OF IW

The ability to easily read other peoples mail, or potentially have your own read raises many legal questions. U.S. relative sophistication in IW compared to all but the most developed economic challengers creates a cornucopia of opportunities in law enforcement, economics, politics and military preparedness. How Machiavellian does the U.S. constitution allow the national security apparatus to be? As with euthanasia and fetal tissue research, information technology has outrun laws and ethics. Until recently, DOD has basically been allowed to work against foreign issues and the FBI has worked the domestic side, with the CIA doing whatever was required. Under this old division of labor DOD didn't need warrants to investigate because it ostensibly did not investigate the activities of U.S. citizens. So why won't the old architecture work? Because information crosses many national boundaries and when an American is discovered to be involved, legal considerations for privacy can become a limiting issue for DOD.

For the last 50 years the U.S. has focused on the USSR and its satellites, and the GCCS served well. The information the US sought emanated from the USSR and it was boresighted by collection agencies. Now the U.S. has the wherewithal to turn attention to all those issues that have been backburner or resulted from the new world disorder, but the targets are different in nature and often more sophisticated. U.S. IW architecture is not presently organized/chartered to maximize its potential. Guidance is adhoc and much that is not wholly legal is probably occurring. The Clinton administration is said to be working on guidance to support the implied IW tasks in the July 1994 National Security Strategy document. For instance, should it be legal for U.S. IW assets to be used in a manner such that a U.S. company obtains a foreign contract as a result, no matter what depth the competitor stoops to? If so, which companies, or segments of the world market, or geographical targets does the U.S. focus on with its superior but not unlimited assets. The opportunities for scandal, national embarrassment and animosity among friends is great, as evidenced by the early March expulsion of six U.S. diplomats by France, which was angered because it claimed that U.S. spying made it lose a lucrative contract. And how does one catch an opponent, or an American proxy who tries to break into a system? With global connectivity the opponent may be a hired gun anywhere in the world representing a militarily unsophisticated, but well advised adversary; the goal may be to bring down international trade if a cause is not recognized. Another example of a challenging IW scenario might involve the laundering of drug money. Current restrictions on DOD IW assets make coordination between IW and enforcement entities awkward and cumbersome when illegal transactions or activities that involve (at least some) Americans crosses national boundaries numerous times. Is a IW "hot pursuit" needed? Better yet, a clearly defined yet flexible set of guidances is needed, soon.

To make matters even more challenging, potential adversaries are obtaining encryption capability that could evaporate many current collection capabilities. Secure phones have been available for several years and are affordable to third world countries, industries, terrorist and would-be traders in contraband of all kinds. Encryption software for personal computers was recently put on Internet by an American computer expert named Philip Zimmmerman. His act may violate U.S. export laws which have sought to protect the capabilities of DOD. These capabilities are so important that the US has pushed the purchase of the "Clipper Chip," which allows U.S. security organizations to monitor communications when needed. The Clipper has been a resounding failure with industry and the public. Zimmerman believes Privacy is as apple-pie as the Constitution, and adds "If you really are a law-abiding citizen with nothing to hide, then why don't you always send your paper mail on postcards?" There is sure to be a legal battle, but the damage has probably been done, and it could only be slowed down a bit by the Clipper Chip. Encryption cripples IW, and to a lesser degree C2W, because finding a signal of interest could eventually become much harder as more systems are used. The biggest problem could be that breaking the information will tie up greater amounts of expensive main frame computer time. The information may take so long to find and break that it will become of marginal use. Billions of dollars of U.S. security investment is at stake.

These issues need careful study as the U.S. is vulnerable and needs to act decisively, yet is on thin ice with respect to the constitution and international law. The best return on IW investment will not occur until all IW participants know their responsibilities and community tactics, techniques and procedures are in place.

THE INTERIM ARCHITECTURE: PHASE ONE

Some sage from a past conflict wrote, "If it looks stupid, but it works, its not stupid." Another asked, "Why reinvent the wheel"? When seeking to provide an interim National Security Architecture, primarily to respond to the IW threat, the hippocratic oath should be the guide; only those changes that reap significant gain should be made, while major reorganizations should be left to a new National Security Act.

The author can offer a series of actions that would provide for greater preparedness for IW. The first goal toward an interim National Security Architecture (after negotiating a plan of action under the cognizance of the National Security Adviser with the backing of the President as discussed earlier) should be to share common databases and communication systems. As stated earlier, work must start in DOD first. One example of a major step toward this goal has been made within DOD by the establishment of MIIDS and Joint Military Command Information System (JMCIS) [7]. The next step would be to fill up databases like MIIDS through production responsibilities that are delegated to the Services and agencies. To use an example from the Intelligence field, the case of MIIDS this delegation has already been coordinated and the guidance promulgated by DIA, but action has been slow. Service Intelligence Organizations are overtaxed and sufficient priority has not been given to this important endeavor that will hasten a quality information pull down capability. Personnel within DOD are adjusting well to the information pull down concept. The Services are still attempting to draw on their own remaining assets to do the specialized support operators came to expect, however, many of those assets have been reduced or provided to the CINC. The Navy and Marine Corps, for example, gave up Fleet Intelligence Center Europe and Atlantic (FICEURLANT) to form Atlantic Intelligence Command (AIC). The resultant inability to satisfy some Service specific needs has caused friction (not unlike that described by Clausewitz regarding war) that often comes with growth and change. The road will smooth as the players adjust to thinking about shared assets and the difference between needs and desires. The Navy may desire strike planning packages to be physically made for a likely target but if they can be held at AIC and accessed when needed via JDISS, the result will be greater efficiency and probably accuracy due to ease of update. More emphasis is needed on Joint databases so that duplication of effort is reduced and a standardized frame of reference can be attained in all areas of IW. Of note, the incorporation of NSA and its databases into a greater IW effort would provide a test case in this phase for the assimilation of quasi-civilian organizations in phase two; the lessons learned would prove valuable.

Data is useless if it cannot be pulled by those who need it. Sufficient communications bandwidth is needed to support systems like MIIDS, JMCIS, JWICS[8] and JDISS[9]. The military is inextricably tied to satellite communications and is now planning for the replacement of existing systems during the period 2005 to 2010 [10]. DOD has accepted major portions of the Navy satellite communication architecture plan shown below for its master plan. The vision brings more efficient, anti-jam/anti-spoof, low-probability-of-intercept EHF capability in the near term; it seeks to capture ongoing technology gains through flexibility in procurement, constellation establishment and broadcast techniques [11].

MIIDS, JDISS, JMCIS, JWICS and the communications to support their use should be made mandatory by DOD/JROC/DIA so that the Services will buy common equipment; this would prevent multiple non-interoperable systems from coming into the Services. Joint operations would be easier because personnel would no longer be unfamiliar with other Services' IW equipment. JDISS is the best example of success in this area [12].

THE INTERIM ARCHITECTURE: PHASE TWO

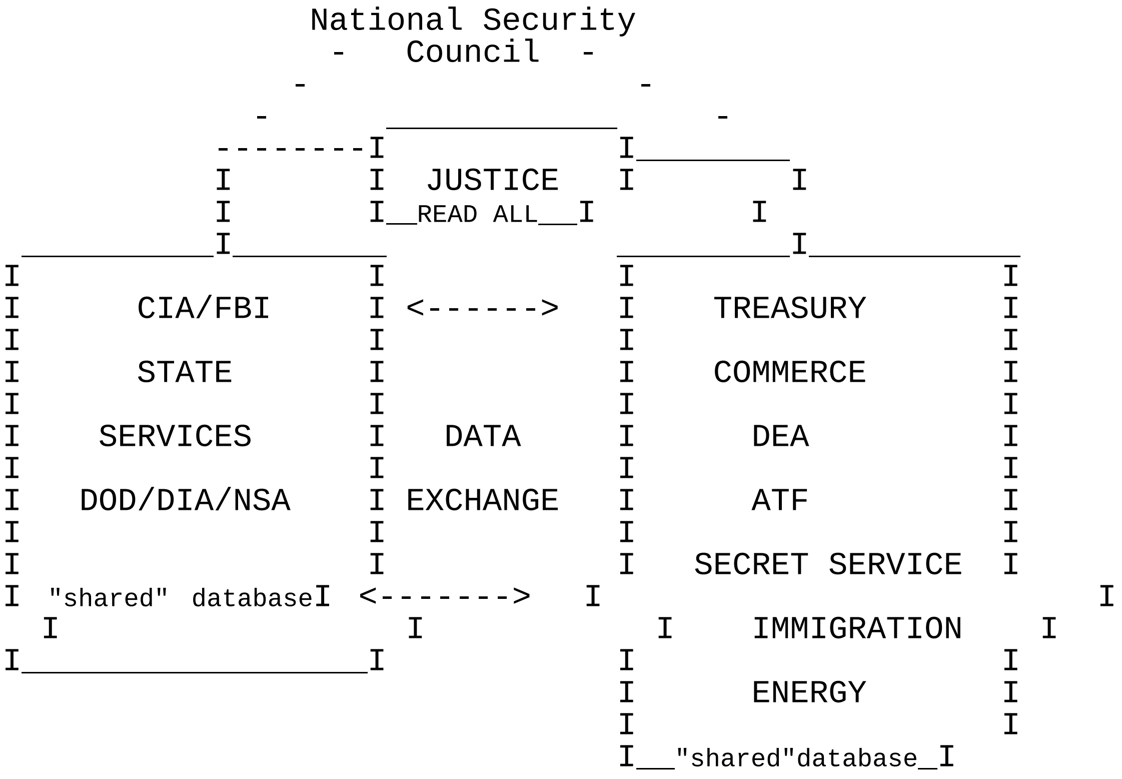
The first step of phase two would be to gradually tie together DOD databases like MIIDS with the databases of non-DOD organizations. Assimilating all non-DOD organizations would be too much too soon. CIA, FBI, and Department of State (DOS) should be included first over a year-long transition. Database security protocols and communication connectivity would be designed to be appropriate to the classification level of information and need to know of particular participants in all organizations. When hardware, software, and personnel adjustments are complete, the remainder of the non-DOD organizations should be connected together in a separate database which allows appropriate data exchange between the two data bases. Participants in a second database would include the Drug Enforcement Agency, Department of Treasury, Secret Service, Department of Justice, Department of Energy, Department of Commerce, Department of Immigration, and the Bureau of Alcohol, Tobacco and Firearms.

The next step in phase two is bold. First, to create efficiencies and ensure unity of effort, the FBI should be subsumed

by the CIA over a two year period following creation of the two main databases and attendant assimilation period. The major missions of CIA and FBI relate to HUMINT and these organizations working together would be more effective against current and future threats to U.S. National Security, most importantly IW. Much of C2-protect in IW is related to HUMINT; to catch a professional IW warrior or terrorist, one must think like him or her and possess the infrastructure to react. While this paper argued in earlier pages that DOD must lead the total IW effort in the beginning, and will continue to lead in the areas of C2-attack, a new CIA must carry the torch of C2-protect. (Consideration should be given to NSA being eventually subsumed by a larger CIA, as NSA's mission is essentially C2-protect through SIGINT.) There would admittedly be some loss of specialized capability with the combination of the CIA and FBI, and great consternation over centering too much power in one organization; afterall, a consideration in the creation of the CIA was to provide a counter-advisory body to the incredible power accumulated at the FBI under President Hoover. The leveling factor that is needed is an empowered Justice Department. An individual (perhaps the Attorney General) or small group within the Justice Department, approved by Congressional vote, would have the ability to have knowledge of all systems and databases in order to ensure American civil liberties are protected and to coordinate legal questions of immediate nature that relate to National Security. This role would be advisory to the President and have special powers of investigation, just as the current Justice Department possesses, but the empowered Justice Department would be able to monitor the operations of all former proprietary organizations. The time for this culture change has come. This step needs to be taken now, but to remove politics from National Security questions, exploration into the establishment of a person or body within Justice that would be permanent is needed. A possible model is the office of the Chairman of the Federal Reserve Board. Current Chairman Alan Greenspan holds a position of no less trust than a Justice Department "Information Czar" would have. A better title, given the current FBI being eventually subsumed by CIA, would be Chairman of the Federal Board of Information (FBI). Confirmation of the Chairman of a new FBI should be as somber a process as that for a Justice of the Supreme Court.

Other less dramatic changes would see NSA brought under closer DOD control in order to increase its relevancy and responsiveness, and greater emphasis on Joint Intelligence by scaling back Service Intelligence in favor of a leaner Defense Intelligence Agency. Service Intelligence personnel should serve most non-operational billets in the Joint arena, either at a Joint Intelligence Center (JIC) or at DIA. As discussed earlier, with today's connectivity, deployed personnel can take advantage of databases, imagery and expert analysis back in the U.S. through systems like JDISS.

The steps outlined in phases one and two would contribute in different ways to greater awareness, capabilities and effectiveness in IW. The National Security Architecture might look similar to the outline below.



CONCLUSION

IW has tremendous potential for U.S. National Security.

Unfortunately, IW also has potential for adversaries if the U.S. does not act with vigilance and decisiveness. The U.S. has tended to use IW in one dimension; the true power of U.S. IW capabilities lies in massing the efforts of all National Security organizations under an overarching Architecture. A U.S. National Security Architecture that connects security organizations must be reorganized and made more responsive in order to stay ahead of the IW threat. Clear, coherent, aggressive policy and doctrine will need to be staffed at the level of the National Security Advisor so that Presidential action can be taken swiftly. Modifications to the current National Security Architecture will ensure coordination between the "producers" and "users" of Information Warfare (IW) support is more responsive. The synergy resulting from DOD and non-DOD governmental National Security organizations, fully coordinating operations, will ensure U.S. dominance of IW. To stay ahead in IW the U.S. must not wait to act, but must move to change, and fully recognize that it is already at war.

BIBLIOGRAPHY

Army Regulation 525-20, "Information Warfare," 09 November 1994.

Army Focus 94, Force XXI, September 1994.

Auster, Bruce B., "Info Wars; When knowledge is Military Power"

US News and World Report, 24 October 94.

CJCS Command and Control Warfare, MOP 30 (Rev. 1 08 March 1993).

Boyd, Austin B. CDR, USN, "Satellite Communications for the 21st Century", Space Tracks, Winter 1995.

Boyd, Austin B. CDR, USN, "Don't Shoot!," Space Tracks, Spring 1995.

Boyd, Morris J., MGen, "Force XXI Op," Military Review, Nov 1994.

Busey, J, B. IV, Adm, "Info War Calculus Mandates Protective Actions, "Signal", Oct 1994.

Campen, Alan D., The First Information War, AFCEA International Press, Fairfax, Virginia, October 1992.

Campen, Alan D., "Intelligence leads Renaissance in Military Thinking, "Signal", August 1994.

Carey, John, "From Internet to Infobahn; The Information Revolution", October 1994.

Clapper, James R., LtGen, and E. H. Trevino, Lt Col, "Critical Security Dominates Information Warfare Moves, Signal, March 1995.

Cohen, Frederick B., "Information Warfare - Concepts and Concerns, The 1st Information Warfare War Game", Presentation by Science Applications International corporation for Office of the Secretary of Defense, December 1993.

Command and Control Warfare, HQ USAF, AFPD 10-17, 12 August 1993.

FM 100-6, Information Ops, Coordinating Draft, HQ USA, 22 July 94.

Handel, Michael, J. "Technological Surprise in War, " Intelligence and National Security, January 1987.

Dixon, James H., "National Security Policy Formulation: Institutions, processes, and issues," National Defense University, 1984.

DOD Directive TS-3600.1, "Information Warfare", 21 December 1993.

Hingtgen, David L., LCDR, USN, "Honing Information Warfare Skills,", Space Tracks, Spring 1995.

Information Architecture for the Battlefield, Office of the Undersecretary of Defense for Acquisition and Technology, October 94.

Jelinek, Michael L., CDR, "Integrated Air and Space Make Every Shot Count," Space Tracks, Winter 1995.

CJCS INST 5118.01, Charter for JC2WC.

Joint Pub 2-0, "Doctrine for Intelligence Support to Joint Operations," Draft June 1991

Joint Pub 3-13, 2nd Draft, Joint Doctrine for Command and Control Warfare (C2W), 01 September 94.

Joint Pub 3-0, Doctrine for Joint Operations, Final Draft.

National Security Strategy of Engagement and Enlargement, The White House, Washington DC, July 1994.

McConnell, J. M., VAdm, "New World, New Callenges, NSA into the 21st Century, " American Intelligence Journal, Spring/Summer 1994.

Naval Doctrine Publication 2, "Naval Intelligence," DON, Office of CNO and HQ USMC, 30 September 1994.

Perry, W. J., Annual Report to the President and Congress, Feb

1995.

Powell, Colin L., Gen, "Information-age Warriors,"Byte, July 1992.

Ryan, Donald E., "Implications of Information-Based Warfare," Joint Forces Quarterly, Autumn/Winter 1994-95, November 1994.

Schwartz, John, "Privacy Program: An On-Line Weapon?," The Washington Post, 03 April 1995.

Sussman, Victor "Gotcha! A Hard-Core Hacker is Nabbed," US News and World Report, 27 February 95.

Toffler, Alvin and Heidi, "War and Anti-War," Little, Brown and Co., 1993.

US News and World Report, "Outlook," 27 February 1995.

END NOTES

1 Historically, those writing on National Security have used the term "structure" to describe the organizations that taken together are tasked with U.S. National Security. The term architecture has become common in recent years, as it better describes the informal lines of communication, tasking and responsibility that exist within and between organizations that today deal with National Security. Information Warfare reinforces, even accelerates the trend toward less structured organizations and groupings of organizations.

Coordination within the National Security Architecture was enhanced in the years following the establishment of the 1947 National Security Act by the use of interagency working groups and working groups and task forces. Within the Information Age, dynamic requirements have forced more responsive reaction to security threats. The National Command Authority needs the right advice quickly. To provide more responsive service, individuals and small groups from different National Security organizations often work together based on Memos of Understanding (MOUs). (An example would be a Central Intelligence Agency (CIA) analyst with special expertise in nuclear technology working with Human Intelligence (HUMINT) capability within CIA, National Security Agency (NSA) capabilities in Signals Intelligence (SIGINT), and with the Department of Energy (DOE) to provide advice to brief the NCA on the advisability of conducting an airstrike on a beligerants nuclear facility.

Today's National Security Architecture must take advantage of C4I improvements and emphasize responsiveness in order to stay ahead of the threat, so that the NCA has the chance of shaping events, but definitely can at least react gracefully to them.

2 Office of the Undersecretary of Defense for Acquisition and Technology, "Information Architecture for the Battlefield," October 94. The Defense Science Board reports...Future "capabilities that are necessary for command and control, for integrated situation awareness to all appropriate levels, for effective support to the shooters, and for effective analysis and training. Information systems of appropriate capacity are required between and among all levels of command to facilitate access to and exchange of information vital to collaborative planning and the effective execution of combat operations. This connectivity is accomplished by highly interactive switched, wideband networks at the higher echelons of command providing interactive video and distributed database transfer capability. Effective command and control among deployed warfighting tactical voice and data networks requires more complex connectivity with narrower band information.

The warfighter should have dynamic control over the information form and flow. He should be able to lay out his information needs tailored to the specific mission. Commanders should be able to specify what information he needs, to what level of detail, at what frequency of update, with which access controls,

with which other information it should be fused, and in what form it should be displayed...

Within the constraints of the current situation, the information officer would then "reprogram the sensor, communications and computing assets to respond to these needs. This capability to reconfigure is not available today. The systems are not capable of being rapidly reconfigured and the tactical staffs do not have the technical capability or necessary tools to do the job. This is and important refocus area for R & D investment."

3 ibid, 2."Corresponding directives are needed to ensure that individual programs have adequate cost an schedule provisions to allow the separate initiatives to achieve full interoperability and a common operating environment. Until a process is put in place to ensure that the joint warfighter's interoperability requirements are considered, these well intentioned but service and agency-unique programs will tend to drift away from migration objectives.

Current acquisition practices exacerbates the tendency to drift since each program is independently supported by mostly independent agencies; a joint corporate perspective is not built into the acquisition process. The warfighting CINC's and JTF commanders have little influence on systems under development or being modified, but they have perhaps the most at stake when systems reach their ultimate application. The joint warfighters' concerns should be represented during the acquisition process to ensure the C4I systems that will support the warfighter, have maintained pace with commercially available technology, and will intermesh well with legacy systems.

Legacy systems must either be migrated into or interfaced with common systems. The motivation to diverge from a common joint interoperation structure is aggravated by the need to maintain compatibility with Service-unique, legacy systems that are not targeted for migration.

There is a need for establishing a process, in a manner akin to that used for the Internet, that identifies incremental improvements and ensures that each can be accommodated and accepted by the other participants. The part of the Internet process that establishes standards, adaptation of commercial products, and distribution of value-added products, has been shown successful. Some variant of that process is appropriate to institute for the DOD. Unlike the DOD, the DOD will need a method of measuring overall cost and benefit of modifications, and ensuring that appropriate benefits accommodate each incremental change. This requires refocused investment to develop and/or acquire tools to facilitate these efforts."

4 The author has extensive experience with JDISS. JDISS is an extremely capable system that allows the transfer and annotation of imagery, serves as a (up to top secret) level message handling system, and can allow two sites to go into a real-time chat mode at top secret level. Communications requirements mandate a minimum 96 kilobyte baud rate to run at an acceptable speed. This very successful system has been deployed throughout the U.S. Government and even to the UN in support of OOTW. JDISS is a fine example of how the planned universal buy of a single system can create significant synergy in operations.

5 Office of the Undersecretary of Defense for Acquisition and Technology, "Information Architecture for the Battlefield," October 94. The Defense Science Board reports "The existing methods for moving and distributing information in the fighting forces are largely hierarchical and sequential. Information flows in a very orderly pattern up and down the operational chain of command. While the new users of information are the regional CINC and JTF commanders, the old patterns of distribution are embedded in doctrine, force structure, and equipment. As a result, the top leadership is well serviced but lower levels are increasingly unable to meet their information needs. There isn't enough access or enough capacity at the lower levels, due to bandwidth limitations as well as equipment and frequency availability."

6 CJC Instruction 5118.01 is the charter for the JC2WC. It states that "the JC2WC mission is to provide direct Command and Control Warfare (C2W) support to operational commanders. The JC2WC will support the integration of the constituent elements of C2W--OPSEC, PSYOP, military deception, EW, and destruction as well as the noncombat military applications of Information Warfare (IW)--throughout the planning and execution phases of operations. This direct support will be provided in the following priority order: joint force commanders (combatant commanders, subordinate unified commanders, and joint task force commanders), Service component commanders, and functional component commanders. Support will also

be provided to OSD, the Joint Staff, Services, USG agencies, NATO, and allied nations. The JC2WC will maintain specialized expertise in C2W-related systems engineering, operational applications, capabilities, and vulnerabilities. The JC2WC, through the Director for Operations (J-3), serves as the principal field agency within DOD for non-Service specific support."

7 The author has extensive experience with Joint Military Command Information System (JMCIS). JMCIS is a C3 support system that functions as a message handling system for secret and below message traffic. Other functions allow the building of graphics to support operational planning up to basic IPB level, a near-real-time display of reporting units (UHF SATCOM), and a operational note ("opnote") function that allows any unit to send a note to another unit in the net. Like JDISS, this system was developed by the Navy and offered to the Joint arena for modification and acceptance as standard Joint C3 gear. Software functionalities of other services has been melded into JMCIS, an example being CTAPS software used by the Air Force to produce the ATO.

8 The author has extensive experience with Joint Worldwide Intelligence Communication System (JWICS) while serving aboard 2nd Fleet Flagship, USS Mt Whitney. JWICS is a secure (to top secret) videoteleconferencing system that allows intelligence personnel to talk face to face regarding difficult issues. The system has turned out to be much more valuable to deployed Commanders to discuss campaign planning, ROE, etc. The system is distributed throughout the world and allows the NCA to talk with CINCs and CJTFs at will, face to face. President Clinton discussed issues over JWICS with the JFC during the Haiti operation. When deployed aboard the USS George Washington, the system was even used by medical personnel to discuss X-rays.

9 The 52nd Director of Naval Intelligence, RADM Thomas A. Brooks, came back to his office in 1991 following an office call with the Chief of Naval Operations and said "We will lead Joint Intelligence." The Navy was the only Service that would give up its best intelligence assets to the Joint arena and was rewarded by the visionary Gen. Colin Powell with command of the major Joint intelligence commands at AIC, JICPAC and JAC Molesworth. The Navy knew Joint was coming and sought to lead rather than have the strength of its very successful, opintel oriented community diluted from the goal of supporting tactical commanders. The Navy continued working toward joint aims by developing JMCIS and JDISS. The author believes these events were watersheds for a tradition-bound Navy that suffered the pain of change early, so that it could position itself solidly behind Jointness and prepare its culture for the future.

10 CDR Boyd in "Satellite Communications for the 21st Century" writes "This unprecedented expiration of space segment requires that Navy and DOD take a fresh look at concepts and technologies, requirements, and resources as plans are made to replenish these

critical communication satellites. In an era of diminishing budgets and burgeoning communication requirements, DOD must find a way to meet more needs with fewer dollars."

[11] ibid 2, "UFO is based on a commercial spacecraft bus, launched on a commercial vehicle, and is managed with a lean minimalist team. The Navy vision is to free the spacecraft supplier to do his job the most efficient way possible, free of strict government control. A second vision is the provision of a follow-on to UFO and MILSTAR in a single constellation. The NAVSPACECOM proposal recommends that a medium launch vehicle class commercial spacecraft be configured with UHF and EHF. This smaller, cheaper (than MILSTAR and UFO) constellation would be deployed with three spacecraft per orbital slot, achieving economy of scale, graceful degradation at end of life, and robust performance in the event of a single or dual bus failure. Among other visions is the provision of a follow-on to DSCS using a commercially procured spacecraft with X-band and direct broadcast capabilities, piping megabits to small antennas (16 inches)...satellite resource management at the CINC, jointly interoperable ground sites, polar EHF communications for operations north of 65 degrees and enhanced EHF packages on UFO are among the other visions..."

[12] The intelligence functions of C4I are leaned on heavily in this paper to show examples of where an IW architecture can be fostered. The author recognizes, and thanks the reader for recognizing that IW success will require migration toward system commonality in all C4I areas. The early success gained in intelligence and communications should be carried over into accomplishments in areas such as sensors, decision support hardware/software, etc. Again, the author would look to JROC to ensure success at the DOD level and a national coordinating body at the inter-agency level.

ABBREVIATIONS

ACTD	Advanced Concept Technology Demonstration
AIC	Atlantic Intelligence Command
ASD (C3I)	Assistant Secretary of Defence for C3I
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
BITF	Battlefield Information Task Force
C2	Command and Control
C2W	Command and Control Warfare
C3	C2 and Communications
C3I	C3 and Intelligence
C4I	C3, Computers and Intelligence
CINC	Commander IN Chief
COTS	Commercial Off The Shelf
CJCS	Chairman, Joint Chiefs of Staff
CJTF	Combined Joint Task Force
CTAPS	Contingency TACS Automated Planning System
DS/DS	Desert Shield/Desert Storm
ELINT	Electronic Intelligence
FLTSAT	Fleet Satellite
FLTSATCOM	Fleet Satellite Communications
GCCS	Global Command and Control System
HF/UHF/SHF/EHF	High/Ultra/Super/Extremely High Frequency
IW	Information Warfare
JAC Molesworth	Joint Analysis Center Molesworth (England)
JC2W	Joint Command and Control Warfare Center
JDISS	Joint Defense Intelligence Support System
JFACC	Joint Forces Air Component Commander
JFC	Joint Force Commander

JICPAC	Joint Intelligence Center Pacific
JMCIS	Joint Military Command Information System
JROC	Joint Requirements Oversight Committee
JTF	Joint Task Force
JWICS	Joint Worldwide Intel Communication System
MIIDS	Military Integrated Intelligence Database System
NDU	National Defense University
NTDS	Naval Tactical Data System
ONI	Office of Naval Intelligence
OPSEC	Operational Security
OODA	Observation, Orientation, Decision and Action
OOTW	Operations Other Than War
MRC	Major Regional Conflict
PGM	Precision Guided Munitions
RDT&E	Research, Development, Testing and Evaluation
PSYOPS	Psychological Operations
SIGINT	Signals Intelligence
STRED	Standard Tactical Recieve Equipment Display
TACS	Tactical Air Control System
TENCAP	Tactical Exploitation of National Capabilities
TRE/TRAP	Tactical Receive Equipment/TRE Applications
UFO	Ultra High Frequency Follow-on

SUPPORTING TECHNOLOGIES FOR IW/C2W
OUTLINE:

DOD information architecture, or Global Command and Control System (GCCS), The GCCS should be reconfigured and improved to allow the flexible and immediate response to OOTW anywhere in the world, but also be robust enough to adequately support, or ramp-up to a totally engaged U.S. military. Changes must be made to the GCCS in cooperation with non-DOD customers, both organizationally and in procurement, to create an overarching U.S. IW architecture.-
BROADCASTS VICE POINT TO POINT COMMS

- VIRTUAL REALITY ISSUES AND TECHNOLOGIES
- OTHER TECHNOLOGIES
- COSMIC STUFF/BLACK PROGRAMS
- TRAINING
- COSTS VICE BENEFITS

Today's communications are more capable and sophisticated, but there are fewer resources. The management of friendly communications has been challenge enough, but the possibilities of IW demands an integrated approach between keeping ones own situational awareness while confusing, deceiving or destroying an adversaries. This responsibility is more, to use a military example, than can be handled by the Communications and Intelligence Officers. To reach maximum potential, IW requires the proper liaison which a functional architecture provides, whether the operation in question is military or otherwise.

While communications probably held its proper place of precedence with respect to funding, importance, etc., during the Cold War, world changes and technological advances have thrust the IW concept to the fore.

GROUND - MOST UNITS WITHIN THE AOA HAVE BEEN ATTRITED TO 50 PERCENT OF COMBAT CAPABILITY

NAVAL - TWO KILO SS REMAIN UNLOCATED. A CRUISE MISSILE SITE LAUNCHED THREE SILKWORMS AT XXXX BUT NO DAMAGE WAS INFLICTED. ANOTHER ? CRUISE MISSILE SITE WAS DESTROYED. COALITION ASSETS DESTROYED ONE ALVAND CLASS DD AND ONE PARVAN CLASS PB IN THE NORTHERN PERSIAN GULF. A SHIP WAS SCUTTLED IN THE PORT OF JASK, WHICH COULD AFFECT G-4 THROUGHPUT IN SUPPORT OF MEF FWD AND FOLLOW-ON OPS.

AIR - THE JOINT FORCE COMMANDER HAS DECLARED ACHIEVEMENT OF LIMITED AIR SUPERIORTY WITHIN THE JOA. IRANIAN MARITIME ACFT REMAIN A MEDIUM THREAT TO NEF/MEF ASSETS AFLOAT. JFACC AIR ASSETS FLEXED TO ATTACK A GROUND UNIT NOTED BY RECON TEAM THAT POSSIBLY WAS TRANFERING CHEMICAL WEAPONS VIA TRUCK (BASED ON TWO BATTALIONS OF INFANTRY PROVIDING SECURITY AND HANDLING THE DRUMS IN MOPP GEAR. FOUR OF FIVE TRUCKS WERE DESTROYED.
OTHER - THREE SCUD WERE FIRED AT MIHAB AIRBASE AND THREE NODONG WERE FIRED AT XXXXX DURING THE 0400Z HOUR. AN END TRAY RADAR WAS NOTED PRIOR TO THE LAUNCH. AN END TRAY EMISSION REPRESENTS THE BEST INDICATOR OF IMPENDING LAUNCH.

ESTIMATE -

12TH INFANTRY DIVISION HQ DR375156

121ST INFANTRY BDE HQ DR720293

1ST BN DR774286 6 81MM
2ND BN DR753289 5 81MM
3RD BN DR736287 7 81MM

122ND INFANTRY BDE HQ

1ST BN
2ND BN
3RD BN

****

11TH ARMORED DIVISION HQ

111TH ARMORED BDE HQ EQ049678

1ST BN (TANK)	EQ055660	05 T-62
2ND BN (TANK)	EQ069697	05 T-62
3RD BN (MECH)	EQ030652	0-3 122MM MTR

4TH BN (ARTY)	EQ071671	1-3 152MM
ARM. RECON CO	EQ053634	2 BMP, 1 BMD

112TH ARMORED BDE HQ EQ058815

1ST BN (TANK)	EQ104798	18 T-62, 1 BMD
2ND BN (TANK)	EQ063801	20 T-62, 1 BMD
3RD BN (MECH)	EQ055827	4 120MM MTR
4TH BN (ARTY)	EQ074824	9 152MM
ARM. RECON CO	UNKNOWN	

113TH MECH BDE HQ UNKNOWN

1ST BN (MECH)	UNKNOWN	
2ND BN (MECH)	UNKNOWN	
3RD BN (TANK)	EQ063933	14 T-62
4TH BN (ARTY)	EQ063924	9 152MM
ARM. RECON CO	UNKNOWN	

114TH ARTY BDE HQ EQ119855

1ST BN EQ106828 8 155MM
2ND BN EQ102840 8 155MM
3RD BN EQ120844 10 122MM MRL

****

13TH INFANTRY DIVISION HQ UNKNOWN

131ST INFANTRY BDE HQ IVO EQ180430

1ST BN IVO EQ130390

2ND BN IVO EQ130440
3RD BN IVO EQ125535

132ND INFANTRY BDE HQ IVO EQ160510

1ST BN IVO EQ160510
2ND BN IVO EQ110410
3RD BN IVO EQ125470

133RD INFANTRY BDE HQ EQ 163273

1ST BN EQ182250
2ND BN EQ190200
3RD BN EQ150235

134 TANK BN EQ030290

135 ARTY BDE HQ IVO EQ210400

1ST BN IVO EQ201315
2ND BN IVO EQ235350
3RD BN IVO EQ201390

105 INDEP PASDARAN ARTY BDE HQ IVO EP490599

1ST BN EP500600
2ND BN EP510585
3RD BN EP520600

106TH INDEP PASDARAN MECH BDE HQ EP299742

1ST BN (MECH) EP304812
2ND BN (MECH) EP303782
3RD BN (TANK) EP305750
4TH BN (ARTY) EP434609

107TH INDEP PASDARAN ARMORED BDE HQ VIC EP410610

1ST BN (MECH) EP436602
2ND BN (MECH) EP465561
3RD BN (TANK) EP400583
4TH BN (ARTY) EP434609

108TH INDEP PASDARAN ARMORED BDE HQ UNK

1ST BN (TANK) IVO EP640550
2ND BN (TANK) IVO EP650530
3RD BN (MECH) IVO EP650565
4TH BN (ARTY) IVO EP740500

193RD INDEP PASADARAN INFANTRY BDE HQ VIC UNKNOWN

1ST BN EP897430
2ND BN EP913466
3RD BN EP891451
4TH BN EP635599 (ARTY)

192ND INDEP PASDARAN INFANTRY BDE HQ UNKN0WN

1ST BN EQ080868 4 120MM MTR
2ND BN EQ063877 3 120MM MTR
3RD BN UNKNOWN
4TH BN UNKNOWN (ARTY)

193RD INDEP PASDARAN INFANTRY BDE HQ UNKNOWN

1ST BN EP897430
2ND BN EP913466
3RD BN EP891451
4TH BN EP635599 (ARTY)

194TH INDEP PASDARAN INFANTRY BDE HQ UNKNOWN

1ST BN EP881451
2ND BN EP881451

3RD BN UNKNOWN
4TH BN UNKNOWN (ARTY)

195TH INDEP PASDARAN INFANTRY BDE HQ UNKNOWN

1ST BN UNKNOWN
2ND BN UNKNOWN
3RD BN UNKNOWN
4TH BN UNKNOWN (ARTY)